Claims

The claims are amended as follows:

1. (Currently Amended) A method for creating a SOAP (Simple Object-Access Protocol) message in web service security using signature encryption, which method is for a sender's creating a SOAP message that includes a SOAP envelope comprised of a SOAP header including a security header and a SOAP body, in web service security based on SOAP message security, the method comprising:

(a) creating a timestamp used to protect against reuse of security information of the SOAP message, and a security token serving as information about security of the SOAP message, and inserting the timestamp and the security token in the security header of the SOAP header, wherein the timestamp includes a creation time and an expiration time of the security information of the SOAP message;

(b) encrypting data to be transferred through the SOAP message with a specific secret key to create encrypted data, and inserting the encrypted data in the SOAP body;

(c) attaching a digital signature to create a signature, encrypting the created signature with the specific secret key to create an encrypted signature, and inserting the encrypted signature into the security header of the SOAP header, so as to prove integrity of the SOAP message and verify identification; and

(d) encrypting the secret key used for encryption of the data and the signature with a public key of a recipient of the SOAP message to create an encrypted key, and inserting the encrypted key in the security header of the SOAP header.

2. (Original) The method as claimed in claim 1, wherein the data and signature encryptions of the steps (b) and (c) are performed according to a symmetric key encryption algorithm.

3. (Original) The method as claimed in claim 1, wherein the encryption of the secret key of the step (d) is performed according to an asymmetric key encryption algorithm.

4. (Original) The method as claimed in claim 1, wherein the encryptions of the data, the signature, and the secret key are performed according to an XML (extensible Markup Language) encryption algorithm.

5. (Currently Amended) A method for verifying a SOAP message in web service security using signature encryption, which method is for a recipient's verifying a SOAP message that includes a SOAP envelope comprised of a SOAP header including a security header, and a SOAP body, in web service security based on SOAP message security, the method comprising:

(a) acquiring a certificate from a security token in the security header of the SOAP header for verifying a signature of the SOAP message;

(b) decrypting an encrypted key in the security header of the SOAP header with a private key of the recipient to acquire a secret key;

(c) decrypting an encrypted signature in the security header of the SOAP header with the acquired secret key, and restoring an original signature;

(d) verifying the restored signature of the step (c) using the certificate acquired in the step (a); and

(e) decrypting encrypted data in the SOAP body with the secret key of the step (b), and restoring original data, wherein the original signature is used to prove integrity of the SOAP message and verify identification.

6. (Original) The method as claimed in claim 5, wherein the step (a) includes acquiring the certificate from a security token in the security header of the SOAP header.

7. (Original) The method as claimed in claim 6, wherein the decryptions of the encrypted signature and encrypted data of the steps (c) and (e) are performed according to a symmetric key encryption algorithm.

8. (Original) The method as claimed in claim 6, wherein the decryption of the encrypted key of the step (b) is performed according to an asymmetric key encryption algorithm.

9. (Original) The method as claimed in claim 6, wherein the decryptions of the encrypted key, the encrypted signature, and the encrypted data are performed according to an XML (extensible Markup Language) encryption algorithm.

10. (Currently Amended) A recording medium with a built-in program, which is used in a method for a sender's creating a SOAP message that includes a SOAP envelope comprised of a SOAP header including a security header, and a SOAP body, in web service security based on SOAP message security, the program implementing:

(a) a function of creating a timestamp used to protect against reuse of security information of the SOAP message and a security token serving as information about security of the SOAP message, and inserting the timestamp and the security token in the security header of the SOAP header, wherein the timestamp includes a creation time and an expiration time of the security information of the SOAP message;

(b) a function of encrypting data to be transferred through the SOAP message with a specific secret key to create encrypted data, and inserting the encrypted data in the SOAP body;

(c) a function of attaching a digital signature to create a signature, encrypting the created signature with the specific secret key to create an encrypted signature, and inserting the encrypted signature in the security header of the SOAP header, so as to prove integrity of the SOAP message and verify identification; and

(d) a function of encrypting the secret key used for encryption of the data and the signature with a public key of a recipient of the SOAP message to create an encrypted key, and inserting the encrypted key in the security header of the SOAP header.

11. (Currently Amended) A recording medium with a built-in program, which is used in a method for a recipient's verifying a SOAP message that includes a SOAP envelope comprised of a SOAP header including a security header, and a SOAP body, in web service security based on SOAP message security, the program implementing:

(a) acquiring a certificate from a security token in the security header of the SOAP header for verifying a signature of the SOAP message;

(b) decrypting an encrypted key in the security header of the SOAP header with a private key of the recipient to acquire a secret key;

(c) decrypting an encrypted signature in the security header of the SOAP header with the acquired secret key, and restoring an original signature;

(d) verifying the restored signature of the step (c) using the certificate acquired in the step (a); and

(e) decrypting encrypted data in the SOAP body with the secret key of the step (b), and restoring original data, wherein the original signature is used to prove integrity of the SOAP message and verify identification.